July 2002 *Issues Paper 07-02*

Business and Security in a Wired World

by COL Dennis Murphy

Background

The U.S. Army War College (USAWC) Center for Strategic Leadership (CSL) conducted a "Business Security in a Wired World" seminar in Rye, New York on 24-25 April 2002. Participants in the event included business executives representing critical infrastructure segments, government officials, and executives of two industry associations. The College's objective in the session was to obtain a better understanding of private sector concerns for information assurance and homeland security. The event featured panel presentations by public and private sector experts in the fields of infrastructure protection and information security. Following the panels, CSL facilitators led a "crisis exercise" which examined key aspects of policy implementation, information sharing, stakeholder expectations, incident response and recovery, and organizational culture. The Army's role in assisting interagency response and the importance of government and private sector partnerships in combating the cyber-threat, was investigated throughout the sessions. In his keynote speech U.S. Representative Curt Weldon, (R-7-PA) applauded the USAWC initiative as a valuable step toward improved understanding and enhanced relations between the government and the private sector.

Seminar Objectives

In the wake of the terrorist attacks on the World Trade Center and the Pentagon on September 11th, 2001 (9-11), government agencies at every level have been re- examining their preparedness to respond to, and ability to recover from, such an incident. Businesses are also re-examining the scope of their exposure and the sufficiency of their risk mitigation and disaster recovery strategies. Now that the unthinkable has happened, contingency plans must be adjusted for catastrophic events that were previously thought too unlikely to take seriously.

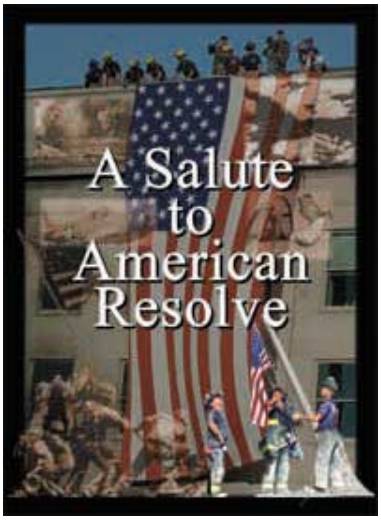
The 9-11 events also served to again highlight the extent of our dependence on Information Technology (IT). The growth of the Global Information Infrastructure (GII) and the incorporation of information technologies into nearly all aspects of daily life led the U.S. Government in 1996 to recognize the need for developing plans to protect the Nation's critical infrastructures. Much has been done in both the public and private sectors to examine the vulnerabilities and begin to formulate solutions. While the attacks were not specifically against IT or communications infrastructure, 9-11 served to further highlight the vulnerabilities of both, the interdependence of the public and private sectors and also to underscore the economic aspects of national security interests.

Government is dependent upon private industry to provide the critical infrastructure through which most government services, including defense communications and logistics, are delivered. Industry, in turn depends on government to provide a level of security for U.S. business interests at home and abroad and also counts on government as a significant customer in many business areas. Several new organizations have been formed to enable the cooperation and information exchange necessary to promote national security in the infrastructure protection arena. President Bush created an Office of Homeland Security to, among other things, coordinate public-private cooperation at all levels and assure that the effort receives presidential attention.

This seminar examined the concepts of cyber terrorism, cyber crime and information infrastructure attacks and fostered an improved understanding of the increasing exposure of U.S. business organizations as targets. The relationship of government and industry in identifying and mitigating critical infrastructure vulnerabilities, and a review of existing, proposed and alternative cooperative strategies was examined as well.

Seminar Design

Seminar panels "primed the pump" in the initial phase of the seminar by discussing current critical issues regarding cyber terror. Armed with this knowledge and their own experiences, participants were then assigned roles as members of government and industry teams in a simulated crisis exercise.



Panels included presentations from the United States Commission on National Security (also known as the Hart-Rudman Commission); the Defense Information Systems Agency; the FBI's National Infrastructure Protection Center; and several leaders in industrial security, describing initiatives designed to mitigate risk, safeguard information, and protect infrastructure.

The crisis exercise, facilitated by representatives from the War College, was designed to draw upon the information provided by the panel experts and examined key aspects of policy implementation, legislative involvement, information sharing, stakeholder expectations, incident response and recovery, and organizational culture. The scenario posited cyber attacks accompanied by physical attacks on two major U.S. corporations (a service corporation and a manufacturing corporation). An inter-governmental, inter-agency response team convened in New York City after the revelation of the cyber attacks. The game also posited an industry-government Joint Crisis Team (JCT) – an operational response entity modeled on the Federal Emergency Management Agency (FEMA)

Federal Response Plan, that put both industry and government resources at the disposal of responders. These four teams (two industry teams and two government teams) grappled with the problems generated by the scenario and interacted with each other, formally and informally, throughout the exercise. The lessons learned include the identification of key organizational and procedural gaps and seams in dealing with cyber terror and information infrastructure attack.

Key Findings

The value of establishing a Joint Crisis Team (JCT) as described above and operating from Washington, D.C. became evident from the early stages of the exercise. The JCT role as an advisory and coordinating body developed in its first interaction with the corporations. Both corporations seemed very open to discuss details of their crisis with the JCT in hopes that the team could help. Requested support included a public relations campaign to limit the damage to the corporations beyond the cyber terror incidents (to include assuaging shareholders). Additionally the corporations requested coordinated intelligence in order to better prepare for the next attack. The JCT's interaction with both corporations allowed it to be the first entity to recognize that the cyber attacks on the businesses were related. Members of the JCT understood the need to gather and pass information to protect national security interests as well as their requirement to pass information to facilitate damage control from a political standpoint. The JCT saw a requirement not only to help the corporations in crisis, but also to be a conduit to coordinate with other industries to arm them with knowledge thereby allowing them to protect themselves. Despite the consensus that the JCT provided important value added during crisis, participants recognized political realities that make the permanent creation of such a team problematic. They noted that these organizations (JCT type) fail because the incentives to industry are wrong. Government can't give financial incentives to business (based on conflict of interest) so psychological buy-in is critical. Business must be made to feel part of the national security solution (government and industry vs. the world instead of government vs. industry). Industry must perceive meaningful participation. The resulting JCT must be lasting. The JCT could be a small standing group of government representatives that can expand and task organize according to crisis. The Department of Commerce should have the government lead because they are perceived as the most palatable to industry.

The corporate teams clearly focused on the immediate need to protect corporate assets, reputation and people as priorities, but saw the government (in the form of the JCT) as an ally to facilitate and support their efforts. This was reflected in their open interaction with the JCT, providing information that would not readily be shared in normal circumstances. (The corporations stopped short of providing personal information on employees when the government attempted to determine whether an insider was the perpetrator. Internally, however, they recognized the need to review personnel reliability screening measures). Both corporations recognized the need for a strong public relations strategy to reinforce that their people were the first priority for the company. Nationally, they launched a campaign reassuring the customer base of the company's capacity to continue operations. Locally this effort included measures both for the public at large (particularly with environmental clean-up concerns) and for the company work force (safety of operations and

care for the employees and their families). Internally they took proactive measures to review and publicize chains of progression within the company, locally, nationally, and internationally. The corporations set aside competitive concerns by notifying associated industrial sectors of the problems being experienced in the company's information technology sector. Interaction with the JCT focused on receipt of governmental notification of impending attacks on the cyber-structure, cooperative exchanges of information (bordering on intelligence) between government and the private sector and requests for phased mitigation procedures for attacks, impending attacks and threats.

Conclusion

Gary Hart and Warren Rudman note in their prescient report of January 2001, "Roadmap for National Security,": "Our challenges are no longer defined for us by a single prominent threat…. Despite the end of the Cold War threat, America faces distinctly new dangers, particularly to the homeland…. These dangers must be addressed." No where is this more true than in the area of cyber terror, where the crisis prevention and response gaps between government and industry remain while there exists a National Critical Infrastructure that inexstricably links both. The "Business Security in a Wired World" seminar revealed that solutions exist. Industry is more than willing to share information with the government in the face of looming cyber terror. They are also willing to be "part of the solution" by partnering with government to form a strategic team to predict and respond to information attacks. National policy makers must take the lead in developing a structure that opens the dialog between industry and government and a standing body that facilitates information flow before and during crisis. While the debate over the scope of the Office of Homeland Security continues, policy makers will be well served to place particular emphasis on this vital area of national security and defense of the homeland.

****
This and other CSL publications can be found online at http://www.carlisle.army.mil/usacsl/index.asp
****